You can enter a value between 1 and 19 (packets). This value defaults to 2. Changes to this value become effective with the next VoIP call.

Note When using adaptive jitter buffers, the minimum jitter buffer size may be less then the value assigned to the `initial-jitter-buffer-size` parameter. Under the appropriate conditions, adaptive jitter buffers may shrink to only one frame in size from the `initial-jitter-buffer-size`.

The following example illustrates how to change the initial jitter buffer size when adaptive jitter buffering is enabled for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set initial-jitter-buffer-size = 5
admin> write
VOIP/{ 0 0 } written
```

For more information on jitter buffer processing see Appendix B, "Determining Jitter Buffer Size."

Type of Service (TOS) or Differentiated Service Codepoint (DSCP) marking

You can set the IP Type of Service (TOS) byte in IP packets that carry signaling messages to define the type of packet marking— either TOS or Differentiated Services Codepoint (DSCP).

For detailed information about how the system supports TOS precedence (RFC 791) and DSCP (RFC 2474) marking of packets, see the *APX/MAX TNT WAN, Routing and Tunneling Configuration Guide.*

Type of Service marking

Type of Service is an eight-bit parameter found in the header of an IP datagram. In networks that support processing of IP packets based on precedence, the Type of Service byte is used to attain a certain level of UDP packet processing by manipulating values for delay, throughput, and reliability.

The `tos-options` subprofile sets the Precedence bits (bit0 - bit2) and the TOS bits (bit3 - bit6) for the Type of Service (TOS) byte use by UDP voice packets. It is divided into three fields, containing the following values:

Bits 0-2: Precedence.

Bits 3-6: TOS (performance cost).

Bit 7: Reserved for Future Use.

0	1	2	3	4	5	6	7
PRECEDENCE			TOS				0

The `tos-options` subprofile is shown below, with default values:

```
[in VOIP/{ 0 0 }:tos-options]
active = yes
precedence = 101
type-of-service = latency
apply-to = both
```

Parameter	Setting
`active`	Enables or disables user configuration of the Type-of-Service byte. Setting this value to yes enables operator configuration of the TOS byte. This is the default value. Setting this value to no disables this feature. Changes to this parameter take effect with the next VoIP call.
`precedence`	Importance of priority of the UDP packet, bit0 through bit2 of the Type-of-Service octet. This is represented by a hexadecimal value, which defines how the network processes the UDP packets. The default is 101. Changes to this value become effective with the next call.
`type-of-service`	Processing attribute management, bit3 through bit6 of the Type-of-Service octet. These bits denote how the network should make trade-offs between throughput, delay, reliability and cost when processing the UDP packets. This value defaults to `latency`. Changes to this value become effective with the next call.
`apply-to`	How the Type-of-Service value is applied to the data flow over the IP network between the MultiVoice Gateways. This parameter has no affect on VoIP call packet processing.

Configuring precedence parameter values

The values assigned to the precedence parameter set bit0 through bit2 of the Type-of-Service octet. The impact of a selected value on UDP packet processing is IP network dependent (see RFC791). You can enter of the following values (hexadecimals), representing processing priorities, as defined by RFC791:

Parameter value	Specifies (RFC 791 definition)
000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	CRITIC/ECP (default)
110	Internetwork Control
111	Network Control

The following example illustrates how to assign a "Flash" precedence or processing priority to UDP packets used for processing VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> list tos-options
```


S 1439

```
admin> set precedence = 011
admin> write
VOIP/{ 0 0 } written
```

Configuring type-of-service parameter values

The values assigned to the `type-of-service` parameter set bit3 through bit6 of the Type of Service octet. The impact of a selected value on UDP packet processing is network dependent (for more information, see "Use of the TOS field in Routing" in RFC1349):

Parameter value	Specifies (RFC1349 definition)
`latency`	Minimize delay
`throughput`	Maximize throughput
`reliability`	Maximize reliability
`cost`	Minimize cost
`normal`	Normal (network control)

The following example illustrates how to set maximized throughput for processing UDP packets used for VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> list tos-options
admin> set type-of-service = throughput
admin> write
VOIP/{ 0 0 } written
```

Differentiated Services Codepoint marking

You can use the IP TOS field in the IP header of packets that carry H.323 signaling messages to set DSCP.

Differentiated services (DS) is an architecture that provides different types or levels of service for network traffic. The differentiated services codepoint is a particular bit pattern (that is, a hexadecimal value) that can be assigned to the DSCP 6-bit field in the IP TOS byte of the IP header. This DSCP field facilitates the definition of future per-hop behaviors.

Implementors should note that the DSCP field is six bits wide. Differentiated Services compliant nodes must select per-hop behaviors by matching against the entire 6-bit DSCP field.

Note The full byte (that is, 8 bits) of the DSCP field can be specified and will be set this way in the IP TOS byte of the IP header. Even though you can set the entire 8 bit in any desired way, only the most significant 6 bits are used and matched to select a Per-Hop Behavior (PHB) by the DS domains in the network. In order to specify traditional TOS/Precedence values, as per RFC 791, the desired bit field can simply be specified as the equivalent DSCP value.

Parameters in voip profile sets DSCP in H.323 packets

You can configure DSCP values for marking H.323 signaling packets by setting the following parameters in the `signaling-tos` subprofile of the `voip` profile:

```
[in VOIP/{ 0 0 }:signaling-tos]
active = no
precedence = 000
type-of-service = normal
apply-to = both
marking-type = dscp
dscp = 00
```

Parameter	Setting
`active`	Enables or disables user configuration of the DSCP. Setting this value to yes enables configuration of the DSCP. This is the default value. Setting this value to no disables this feature. Changes to this parameter take effect with the next VoIP call.
`precedence`	Importance of priority of the UDP packet, bit0 through bit2 of the Type-of-Service octet. This is represented by a hexadecimal value, which defines how the network processes the UDP packets. The default is 000, which means Normal Priority. Changes to this value become effective with the next call.
`type-of-service`	Processing attribute management, bit3 through bit6 of the Type-of-Service octet. These bits denote how the network should make trade-offs between throughput, delay, reliability and cost when processing the UDP packets. This value defaults to `normal`. Changes to this value become effective with the next call.
`apply-to`	How the Type-of-Service value is applied to the data flow over the IP network between the MultiVoice Gateways. This parameter has no affect on VoIP call packet processing.
`marking-type`	Either precedence-tos or dcsp. When set to dscp, Differentiated Services CodePoint marking (RFC 2474) can be set by entering a hexadecimal number via the dscp parameter. The differentiated services codepoint is a particular bit pattern (that is, a hexadecimal value) that can be assigned to the Differentiated Services Codepoint (DSCP) 6-bit field in the IP TOS byte of the IP header. When set to precedence-tos, the system marks packets in a manner consistent with RFC 791.

Parameter	Setting
dscp	The DSCP tag to be used in the marking of the packets (if the `marking-type` parameter = dscp). Hexadecimal field, 1 byte. The default value is 00 and the range is from 00 to `ff` hexadecimal.

For example, the following commands enable DSCP marking and specify a value of 33 for H.323 signaling packets:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set signaling-tos active = yes
admin> set signaling-tos dscp = 33
admin> write
```

For details about configuring DSCP marking in SS7 signaling packets, refer to your platform's *Physical Interface Configuration Guide*.

Controlling VoIP call volume

The `maxcalls` parameter controls the maximum number of VoIP calls a TAOS unit can process simultaneously, by limiting the number of digital signal processors (DSPs) available for processing VoIP calls.

Note When the `voip-max-capacity-allowed` parameter is enabled and licensed for an APX in the read-only base profile, the `maxcalls` parameter is automatically set to the maximum number of VoIP calls that can be processed (for example, 2688). (See "Base profile parameters" on page 2-2 for details.)

Limited DSP availability is useful when continued high call volumes on a network affect the call quality. Adjusting the value for `maxcalls` allows a TAOS unit to allocate more system resources to processing fewer calls, resulting in improved call quality. When active calls exceed the resources that are available to process VoIP calls, the caller hears a busy signal from the TAOS unit.

Maxcalls parameter

The following example illustrates how to limit the number of available DSPs to handle VoIP calls:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set maxcalls = 128
admin> write
VOIP/{ 0 0 } written
```

You may enter any number between 1 and the maximum value. On a MAX TNT, the `maxcalls` parameter defaults to 672—only values between 1 and 672 can be entered. On a APX, only values between 1 and 2688 can be entered. If an APX has only been licensed for up to 2688 calls, and it receives call attempt #2689, the call will be rejected.

Changes to this parameter become effective with the next call.

Note This value does not reflect actual VoIP call volumes achieved by the TAOS unit in either a testing or production environment.

Exceeding the maximum call volume

When the licensed call volume is exceeded, a MultiVoice Gateway displays the following warning message if debugging and the h323warn command (level 2 or higher) were enabled:

```
H323:   4: WARNING: _wanNewCall():
... call denied due to simultaneous call capacity
... 2689 > 2688
```

Configuring H.323 (v2) fastStart

The H.323 (v2) fast connect procedure allows for faster call completion. Fast connect provides faster call setup and with fewer round-trip connections needed to establish a call between end points.

H.323 (v2) defines a fast connect procedure, which is also known as *fastStart*. This fast connect procedure streamlines the connection establishment of calls when:

- Capabilities exchange is not necessary.
- End point compatibility is assumed.

H.245 capabilities exchange is performed *after* the fast connect procedure is completed, because the logical channel set-up exchange is embedded in the H.225 message exchange. However, open logical channel exchange is not performed.

With fast connect, messaging can be collapsed into a single handshake consisting of a setup message and a connect message.

fastStart vs. standard H.245 procedure

The fast connect procedure results in much faster call setup in the network than that provided by the standard H.245 procedure. In situations in which fast connect is unsuccessful, the call is automatically set up using standard H.245 procedures instead.

Upon completion of the fast connect procedure, to set up a voice call, the H.245 procedure is initiated and all mandatory H.245 procedures need to be completed using either H.245 tunneling or H.245 connection. This is especially important if you use a third-party gateway that does not support the fallback condition. In this case, the call will be released due to H.245 time-out.

H.323 (v2) fast connect call flow

The following call flow occurs when H.323 (v2) fast connect is used.

The calling end point sends a setup message to the called end point. The setup message contains a fastStart element with the following audio mode information:

- Codec
- Rate
- RTP/RTCP addresses

If the called end point initiates the use of the fast connect procedure for the call, the called end point may return information in the call proceeding, call alerting, and call connect messages that contain a fastStart element.

If the called end point fails to initiate the use of the fast connect procedure, the called end point may respond with a call proceeding, call alert or call connect message that does not contain a fastStart element.

If the calling end point receives call proceeding, call alert, or call connect messages without a fastStart element, the calling end point terminates the fast connect procedure. The calling end point also completes the H.245 procedure, using one of the following two methods:

- H.245 tunneling, provided that H.323 tunneling is supported at both end points.
- A separate H.245 channel.

Reverting to the H.245 connection

When fast connect is being used, either end point can initiate a separate H.245 connection at any time. Initiation of an H.245 connection is required under either of the following conditions:

- If either end point does not support the fastStart element and H.245 tunneling.
- If a call uses the fastStart element and if H.245 tunneling is not supported for the call.

When either end point initiates a separate H.245 connection, this supports:

- Fax transmission.
- Invoking the call feature that require the use of H.245 procedures such as Out-of-Band (OOB) DTMF.

H.245 call flow

All mandatory H.245 protocol elements that normally occur upon initiation of an H.245 connection are completed prior to initiation of any additional H.245 procedures. These include:

- Cap exchange
- Master/slave determination

Note The media channels that are established as a result of the fast connect procedure are inherited as though they had been opened using normal H.245 `OpenLogicalChannel` and `OpenLogicalChannelAck` procedures. For such inheritance to succeed, media sessions opened during the fast connect procedure must use only well-known sessionID values, as defined in the H.245 standard.

Using fastStart with H.245 tunneling

When a fastStart element is being used, either end point can initiate the use of H.245 tunneling. H.245 tunneling is required under either of the following circumstances to:

- Support the fax transition.
- Invoke call features that require the use of H.245 procedures.

A calling end point can also include both a fastStart element and can set the `h245Tunneling` field to `TRUE` within the same setup message. Similarly, a called end

point can include a fastStart element and set the `h245Tunneling` field to `TRUE` within the same Q.931 response. In this instance, the fast connect procedures are followed, and the H.245 connection is not established until the actual transmission of the first tunneled H.245 message has occurred, or until the separate H.245 connection has been opened.

Note In the H.323 (v2) standard, the calling end point must include one but *not* both of the following in the same setup message:

- A fastStart element.
- An encapsulated H.245 messages in H245Control.

The presence of the encapsulated H.245 message in this instance overrides the Fast Connect procedure.

Terminating the H.323 V2 Fast Connect Procedure

The Fast Connect procedure is terminated when one of the following events has occurred:

- An encapsulated H.245 message is sent.
- A separate H.245 connection by either end point prior to the sending of a Q.931 message containing fastStart by the called end point is initiated.

faststart-enable parameter

The `faststart-enable` parameter enables and disables the fastStart feature. If the `faststart-enable` parameter is enabled (set to yes), the fast connect procedure is initiated. yes is the default value.

The following procedure illustrates how to enable fastStart:

```
[in VOIP/{ 0 0 } read]
admin> set faststart-enable=yes
admin> wri
```

Configuring H.323 call management parameters

A TAOS unit may be configured to use IPDC in support of an SS7 network configuration or use H.323 in support of non-SS7 networks. TAOS units use the following parameters to handle H.323 management:

- `gatekeeper-ip`
- `gatekeeper-ip-sec`
- `gatekeeper-keepalive`
- `registration-retries`
- `registration-retry-timer`
- `primary-retries`
- `cut-thru-enable-nearend`
- `dtmf-tone-passing`
- `clid-suppress`
- `call-keep-alive-timeout`
- `call-inter-digit-timeout`

- `true-connect-enable`
- `single-dial-enable`
- `call-hairpin`
- `vpn-mode`
- `h323-voice-ann-enabled`
- `voice-ann-dir`
- `voice-ann-enc`
- `g711-transparent-data`
- `trunk-quiesce-enable`
- `early-ringback-enable`
- `trunk-prefix-enable`
- `rtpqos-polling-enable`

These parameters can be ignored or reset when using IPDC to route VoIP calls from an SS7 network. When operating in an H.323 environment, the only parameter that must be set is the `gatekeeper-ip` parameter. This identifies the location of the H.323 gatekeeper system that performs call management for the MultiVoice network.

Note The use of the H.323 `voice-ann-enabled`, `voice-ann-dir`, and `voice-ann-enc` parameters is discussed in Chapter 4, "Voice Announcement Administration." The use of the `rt-fax-options` subprofile is discussed in Chapter 5, "MultiVoice Real-time Fax."

H.323 gatekeeper communication

An H.323 gatekeeper manages the MultiVoice network. It provides address translation and controls access to the local area network for all TAOS units processing VoIP calls and any H.323 terminals (such as, PCs running H.323-compliant telephony software). All gatekeeper functions are performed by the MultiVoice Gatekeeper running MVAM software.

Identifying the primary gatekeeper

The `gatekeeper-ip` parameter identifies the computer running MVAM that performs all the H.323 gatekeeper functions for this TAOS unit when MultiVoice is configured to perform H.323 call processing.

MultiVoice implements the H.323 direct call model for VoIP networks, so each TAOS unit must communicate with a gatekeeper to perform call registration and admission, and report statuses (RAS). The TAOS unit sends all call request messages and call processing information to the IP address specified by `gatekeeper-ip`.

After changing the default value of `0.0.0.0` to an IP address, you need to reset the TAOS unit. Changes to this parameter take effect with the next registration cycle.

Note The `gatekeeper-ip` parameter must be configured for a TAOS unit to start processing VoIP calls in an H.323 network.

The following example illustrates how to set the IP address of MVAM that functions as the H.323 gatekeeper for this TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
```

```
admin> set gatekeeper-ip = 123.123.23.1
admin> write
VOIP/{ 0 0 } written
```

The TAOS unit must be able to send packets to and receive packets from MVAM. You can verify connectivity by pinging the IP address of MVAM from the terminal server. If the pings fail, see your network administrator about possible routing problems.

Identifying a secondary gatekeeper

The gatekeeper-ip-sec parameter identifies a second computer running the MVAM software that performs all the H.323 gatekeeper functions for the TAOS unit when configured for H.323 call processing, if it can't register with the gatekeeper identified in the gatekeeper-ip parameter.

The following example illustrates how to set the IP address designating the MVAM that functions as the secondary H.323 gatekeeper for this TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set gatekeeper-ip-sec = 123.123.23.13
admin> write
VOIP/{ 0 0 } written
```

The following dependencies apply:

When an IP address is not assigned to gatekeeper-ip-sec, then the TAOS unit goes into a *slow poll mode* with the MultiVoice Access Manager at gatekeeper-ip. The TAOS unit attempts registrations at 30-second intervals with MVAM as defined by the gatekeeper-ip parameter. During the time the gateway is unregistered, new calls are *blocked*, which means the TAOS unit rejects any new calls.

Anytime a TAOS unit attempts to register with a gatekeeper, that gateway is effectively unregistered with any gatekeeper. During this period, calls are blocked. However, existing calls continue to operate normally.

The TAOS unit must be able to send packets to and receive packets from MVAM. You can verify connectivity by pinging the IP address of MVAM from the terminal server. If the pings fail, see your network administrator about possible routing problems.

Setting gateway registration policy

Registration is a process where the TAOS unit informs MVAM of its identity and availability to process VoIP calls. The transport address and alias address of the TAOS unit across the RAS (registration, admission and status) channel to MVAM. Sending the transport and alias addresses must take place initially before the TAOS unit can connect calls and repeats periodically.

The TAOS unit sends a Registration Request (RRQ) to MVAM. TAOS units used as MultiVoice Gateways send information about the feature set installed on the MVAM as part of each Registration Request (RRQ) message. This allows MVAM to distinguish between MultiVoice Gateways running TAOS 10.0 and previous releases to provide appropriate call processing support for each MultiVoice Gateway.

MVAM responds with either a registration confirmation (RCF) or registration reject (RRJ) message. Once registered, the TAOS unit can request address translation, admissions control and zone management services from the MVAM.

Controlling keepalive registration

Once registered with a gatekeeper, a TAOS unit re-registers with its currently registered gatekeeper every 120 seconds. This is called the *keepalive registration*. The gatekeeper-keepalive parameter sets the time interval between attempts to reregister with a system running MVAM, following the initial registration. The parameter value equals the wait time, in seconds, between each attempt to reregister.

You can enter any value between 1 and 65535. Changes to the gatekeeper-keepalive parameter become effective with the next registration cycle.

The following example illustrates how to set the keepalive time interval for a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set gatekeeper-keepalive = 120
admin> write
VOIP/{ 0 0 } written
```

Note If you change this parameter, you should also change the registrationDuration parameter on MVAM. Gateway registration with MVAM automatically expires within that time frame.

Detecting gatekeeper failure

At H.323 stack initialization time, a TAOS unit attempts to register with the primary H.323 gatekeeper. The H.323 stack does not initialize when the primary gatekeeper is not configured. Registration with a primary gatekeeper fails when the gateway cannot register with the primary gatekeeper after all attempts have been made. By default, a TAOS unit makes five registration attempts at 5-second intervals.

When registration with the primary gatekeeper fails, a TAOS unit attempts to register with the secondary gatekeeper if there is a valid address (non-null) configured for the gatekeeper-ip-sec. The TAOS unit applies the same registration policy (five registration attempts at 5-seconds intervals). Once it successfully registers with the secondary gatekeeper, the TAOS unit operates in *backup mode*.

If there is no valid address (null) configured for the gatekeeper-ip-sec when the primary gatekeeper fails, then the TAOS unit goes into slow-poll mode with the MultiVoice Access Manager identified by the gatekeeper-ip parameter setting.

Setting reregistration policy

After a TAOS unit registers with the MultiVoice Access Manager identified in the gatekeeper-ip-sec parameter setting, it periodically attempts to reregister with the primary MVAM identified in the gatekeeper-ip parameter setting. The attempts to reregister with the primary gatekeeper are initiated after every cycle of five successful registrations with the secondary gatekeeper. If the gateway cannot register with the primary gatekeeper in this mode, it performs keepalive registration with the secondary gatekeeper.

Setting the number of registration attempts for each cycle

The registration-retries parameter sets the number of attempts a TAOS unit makes each time it executes keepalive registration. Since a gateway might not successfully register on its first attempt, the value for this parameter represents the

number of repeated registration attempts a gateway makes during a registration cycle, until it either registers successfully or until all attempts have failed.

You can enter any value between 1 and 200 for the `registration-retries` parameter. Changes to this value become effective with the next registration cycle. This value defaults to 5 attempts.

The following example illustrates how to set the number of registration attempts a TAOS unit performs during a registration cycle:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set registration-retries = 5
admin> write
VOIP/{ 0 0 } written
```

Setting the interval between registration attempts for each cycle

The `registration-retry-timer` parameter sets the time interval between each registration attempt with MVAM. The parameter value sets the pause, in seconds, between each registration attempt specified by the `registration-retries` parameter.

You can specify a time between 1 and 200 seconds. Changes to this value become effective with the next registration cycle. This value defaults to 5 seconds.

The following example illustrates how to set the time interval between each registration attempt specified by the `registration-retries` parameter:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set registration-retry-timer = 5
admin> write
VOIP/{ 0 0 } written
```

Setting the number of reregistration attempts

The `primary-retries` parameter sets the number of attempts a TAOS unit makes whenever it tries to reregister with the MultiVoice Access Manager identified in the `gatekeeper-ip` parameter setting. Since a gateway might not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a gateway makes during a reregistration cycle, until it either registers successfully with the MultiVoice Access Manager identified by the `gatekeeper-ip` parameter setting or until all attempts have failed.

Setting `primary-retries` to zero (0) disables this feature. You can enter any value between 0 and 200. Changes to this value become effective with the next registration cycle. The default value is 1.

The following example illustrates how to set the number of registration attempts this TAOS unit will execute when attempting to reregister with MVAM at `gatekeeper-ip`:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set primary-retries = 5
admin> write
VOIP/{ 0 0 } written
```

Reporting trunk capacity to the gatekeeper

For all T1 or E1 trunks attached to a MultiVoice Gateway, the gateway can report the following information to MVAM:

- Trunk status at initialization
- Changes in trunk status after initialization
- Trunk profile changes after initialization
- Trunk group changes after initialization

Changes in trunk availability are reported for both VoIP and data trunk calls as part of the nonStandardData byte sent in subsequent registration request (RRQ) messages.

A MultiVoice Gateway periodically reports trunk availability to MVAM in response to an information request (IRQ) message and as part of a subsequent registration request (RRQ) message. The nonStandardData byte uses two data fields for reporting trunk status for all enabled trunks and changes to trunk status. MVAM extracts this information to determine which trunk groups have available channels for egressing VoIP calls.

When a MultiVoice Gateway is initialized, it sends a full RRQ to MVAM, reporting the status of all enabled trunks. When trunk group routing is enabled for VoIP calls, the trunk status information allows MVAM to identify available channels for egressing VoIP calls.

A lightweight RRQ reports only changes to the original trunk information. This message is issued in response to an IRQ message from MVAM and in a subsequent RRQ message. The RRQ message reports the following information:

- Any changes in trunk statuses (such as an active trunk going down, or an inactive trunk coming up), as they occur. An RRQ is sent immediately for just the changed trunk, even if that trunk is disabled.
- Any changes made in T1 or T3 profile parameter values (such as changes in signaling mode, default call type, etc.), that affect trunk availability. An RRQ is sent immediately for just the profile change. However, if the change is to the `t1:line-interface enabled` parameter, this is reported as a change in trunk status, not a profile change.
- Whenever the assigned trunk group usage changes for a trunk or channel. An RRQ is sent immediately for only the enabled trunks. Disabled trunks are NOT included in the report.
- Any changes in channel statuses (such as an active trunk going down, or an inactive trunk coming up), as they occur. Every lightweight RRQ automatically reports channel status changes when the status of any channel differs from the status previously reported. Only the channel status at the time the RRQ is generated matters. The channel status changes that occur between scheduled keepalive registrations are not reported.

In the absence of trunk or profile changes, for every lightweight RRQ sent by the MultiVoice Gateway during keepalive registration channel the status is checked and compared. Disabled trunks are also included in the RRQ sent during keepalive registration.

H.323 call signaling

During each VoIP call, a TAOS unit processes a variety of call signaling operations. These operations include

- Passing and responding to call-progress signals
- Delaying transmission of call-progress signals to the PSTN
- Passing and processing DNIS/ANI/CLID
- Performing call keepalive signaling with distant end points
- Enabling transparent processing of fax/modem signals

Controlling call-progress tones on a local gateway

For MultiVoice networks using non-PRI trunks, there is an answer supervision feature. The `cut-thru-enable-nearend` parameter enables call-progress tones from the distant PSTN to be passed across the IP network to the local TAOS unit. When enabled, the near-end TAOS unit in a VoIP call plays call-progress tones from the PSTN on the far-end out-dialed DS0. When disabled, the far-end TAOS unit locally generates call-progress tones. The result is that this feature allows callers at either end of a MultiVoice call to hear the call-progress tones from the distant PSTN.

Enabling call-progress tones provides answer supervision support for TAOS units using non-PRI trunks, by processing the call-progress tones from the distant PSTN. Using far-end cut-through, the tones from the PSTN on the far-end, out-dialed DS0 are passed back to the near-end gateway via RTP and made available for play before the call is actually setup. You can enter either of the following values:

Parameter value	Specifies
yes	(Default) That the near-end TAOS unit plays call-progress tones from the far-end out-dialed DS0. PSTN-generated call-progress tones are passed across the IP network, using RTP packets between gateways. The audio signals from the distant PSTN are compressed by the far-end gateway for transmission across the IP network, then decompressed by the near-end gateway and played for the caller.
no	That this feature is disabled. The near-end TAOS unit ignores the RTP audio signaling and attempts to play back local progress tones in response to Q.931 messages.

Changes to this value become effective with the next call.

The following example illustrates how to enable local call-progress tone cut-through for VoIP calls on a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set cut-thru-enable-nearend = yes
admin> write
VOIP/{ 0 0 } written
```

The following dependencies apply to using the `cut-thru-enable-nearend` parameter:

- Network traffic volumes and voice quality determine when this parameter value should be modified. When call volumes increase, disabling this feature can improve call performance.
- When no is selected, callers hear silence until the local TAOS unit generates call-progress tones in response to Q.931 messages.

Note The fast H.245 (start H.245 before Q.931 CONNECT) is always used and has no impact.

Controlling transmission of call-progress tones to the PSTN

MultiVoice can delay transmission of call-progress tones to the PSTN until the call is answered. Delayed transmission avoids incurring PSTN charges for a call that is connected end-to-end across the VoIP network.

A MultiVoice Gateway can be configured through the command-line interface to delay sending the connect message to the ingress PSTN switch until the following information is received from the egress MultiVoice Gateway:

- An H.323 alerting message
- A call-progress message from the egress PSTN indicating the call has been answered

Previously, incoming VoIP calls from the PSTN were connected at the near-end gateway before any H.323 signaling was sent to the far-end gateway. As a result, a PSTN charge was incurred at the time the call connected to the near-end gateway, before the called party received and answered the call from the far-end gateway. This is called a true connect call.

True connection requires a default call type of voip on T1 or E1 trunks accepting incoming VoIP calls, as illustrated by the following:

```
[in T1/{ shelf-1 slot-10 1 }:line-interface]
default-call-type = voip
[in E1/{ shelf-1 slot-11 1 }:line-interface]
default-call-type = voip
```

The true-connect-enable parameter allows the operator to force the TAOS unit to delay alerting the PSTN, when applicable, and to send connect messages only when the equivalent H.323 messages are received. No PSTN charge is incurred unless the H.323 VoIP call is connected.

Note True connection does not work for E1 R2/R1 trunks. Use this feature only with T1-inband, T1-PRI, or E1-PRI trunks.

The true-connect-enable parameter may be assigned the following values:

Parameter value	Specifies
yes	An alerting message is sent to the ingress PSTN switch only when an H.323 alerting message is received on the ingress VoIP gateway, and a PSTN connect message is sent only when the H.323 VoIP call has been answered. This ensures that no charges are incurred for incomplete calls.

S 1452

Parameter value	Specifies
no	(The default) An alerting message is sent to the ingress PSTN switch as soon as the connection is established with the ingress MultiVoice Gateway. This behavior results in the caller incurring a PSTN charge at the time of connection to the near-end gateway, before the called party has received and answered the call from the far-end gateway.

The following commands configure delayed PSTN alerting and connect messages (true connect signaling) on a TAOS unit:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set true-connect-enable = yes
admin> write
VOIP/{ 0 0 } written
```

The following dependencies apply to the true-connect-enable parameter:

- The default-call-type parameter in the t1:line-interface or e1:line-interface sub-profile must be set to voip for T1 or E1 trunks used for incoming VoIP calls that require true connect signaling. Setting this parameter to voip causes *all* calls received on the trunk to be mapped to VoIP.
- The T310 timeout includes the time that the called party's phone is ringing, so a 10-second timeout can cause the near-end gateway to tear down the call too soon. With ISDN trunks, set T310 on the Telco switch or PBX to 30 seconds or greater when using the true connect feature.
- When the true connect feature is enabled and a VOIP call fails before the PSTN call is fully connected, the gateway is still able to send an appropriate tone or voice announcement to the caller.

Processing call failures

Call failures are reported for incoming PSTN calls by playing the appropriate tones or announcements to alert the caller of the call failure prior to connecting the call across the MultiVoice network. The ingress TAOS unit will only tear down the call after playing the proper tone or announcement to let the user know that the call failed.

Rerouting DTMF signals

Out-of-band processing of DTMF packets sends digits and tones received from the PSTN, by the near-end TAOS unit, across the network using non-UDP packets. When these packets reach the far-end TAOS unit, they are regenerated for use by the MultiVoice application or sent out to the PSTN.

DTMF tones may be degraded or distorted when they are encoded and decoded as part of the voice stream. Degradation and distortion results from the design of the audio codecs, which are intended to process speech and not DTMF tones. Consequently, DTMF input may not be detected by the far-end gateway or PSTN.

S 1453

This `dtmf-tone-passing` parameter enables filtering the tone from the voice path and passing the corresponding digits to the far-end gateway using a non-RTP path. Once received at the far end, the digits are played out.

This out-of-band processing works even with both gateways operating in opposite modes. For example, when an inband gateway is talking to an out-of-band gateway, the inband gateway will accept the out of band DTMF play-out commands. You can enter one of the following values:

Parameter value	Specifies
`dtmf-tone-passed-inband`	(Default) That the near-end TAOS unit passes PSTN-generated DTMF digits and tones as part of the voice processing stream. These tones will be compressed by the selected audio codec and transported across the IP network using UDP packets.
`dtmf-tone-passed-outofband`	That the near-end TAOS unit passes PSTN-generated DTMF digits and tones across the network using non-UDP packets. Once received at the far end, the digits are played out to the local PSTN/caller.
`rtp`	DTMF tones are transferred and passed via the same channel to the decoding DSP, according to the RFC2833 standard. By following the RFC2833 standard, DTMF carriage in the Real-time Transport Protocol (RTP) header allows packet calls to use a non-inband DTMF tone passing mode. There is no negotiation of support for RFC2833 at call setup time. Therefore all machines in a network must support RFC2833 for any one of them to use it. **Note** Support for RFC2833 is provided only for the G.711 and G.729(A) voice codecs. Future releases may implement RFC2833 support for the more complex and higher compression codecs (such as, G.723.1)

Changes to the `dtmf-tone-passing` parameter are effective with the next VoIP call.

To enable out-of- band DTMF processing for VoIP calls on an TAOS unit, set the `dtmf-tone-passing` parameter as follows:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set dtmf-tone-passing = dtmf-tone-passed-outofband
admin> write
VOIP/{ 0 0 } written
```

Blocking Caller ID on a local gateway

MultiVoice administrators can block Caller ID at the destination gateway by preventing the Calling Line IDentification (CLID) string from being passed to the PSTN and the ultimate called destination. Certain carrier switches, which do not recognize the CLID sent from an inbound gateway, might subsequently reject outbound calls when they received the Caller ID from an outbound gateway. The switches expect the Caller ID to be the subscriber number configured by the subscriber-side PRI/BRI (MultiVoice supports only subscriber side ISDN).

The `clid-suppress` parameter blocks transmission of the caller's CLID to the PSTN. Blocking CLID transmission prevents switches from rejecting calls as a result of the Caller ID inconsistency and allows service providers to control and charge for Caller ID services.

You can enter either of the following values:

Parameter value	Specifies
yes	The local TAOS unit blocks transmission of the Caller ID (CLID) signals received from the distant TAOS unit, excluding from the data passed to the local PSTN.
no	(Default) That the local TAOS unit transmit the Caller ID (CLID) signals received from the distant TAOS unit, passing it to the local PSTN.

Changes to this parameter are effective with the next VoIP call.

To block outbound Caller ID on a MultiVoice Gateway, proceed as follows:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set clid-suppress = yes
admin> write
VOIP/{ 0 0 } written
```

Enabling keep alive registration between calling end points

TAOS units can determine whether a call's remote end point (such as gateway, terminal, PC, etc.) has become unreachable. A TAOS unit can subsequently terminate the connection.

The `call-keep-alive-timeout` parameter controls how often a MultiVoice Gateway polls a remote gateway or client during a VoIP call to verify that it is still functioning and reachable over the IP network. The same parameter setting specifies the time in which the remote gateway or client must respond before the call is dropped.

When the value of this parameter is set between 1 and 32767 (seconds), a keepalive packet is sent at regular intervals to the remote gateway or client. If no response is received, the call with that end point is dropped. If the call is dropped, the gateway sends a Drop Request (DRQ) message to the MVAM with the disconnect reason of "`forcedDrop`." When this parameter's value is 0, the default, this feature is disabled. Changes to this parameter take effect with the next VoIP call.

To enable keep alive registration on a TAOS unit for VoIP calls, proceed as follows:

S 1455

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set call-keep-alive-timeout = 150
admin> write
VOIP/{ 0 0 } written
```

Note Enabling keepalive registration only works with other MultiVoice Gateways and selected PC and terminal end points that are H.323 compliant. This feature is normally not used.

Enabling transparent fax/modem operations

MultiVoice Gateways can process fax/modem traffic over a VoIP channel, regardless of which audio codec is currently in use. A MultiVoice Gateway can detect a fax/modem transmission on a VoIP channel and enable fallback to the G.711 audio codec to allow transparent processing of fax/modem transmission. Detection of fax/modem is based on an algorithm that listens for an Answer tone. generated by an answering fax/modem. The Answer tone is significantly different for high-speed modems and fax terminals. The difference in Answer tones allows a MultiVoice Gateway uses to discriminate between the two types of equipment. Typically both real-time fax and transparent data can be enabled simultaneously.

To work, this feature must be enabled on MultiVoice Gateways at either end connecting the fax/modem call. Both MultiVoice Gateways must agree to transparent mode before the call bandwidth is increased to G.711 bandwidth, 64Kbps.

Using transparent modem with real-time fax

If a TAOS unit has been licensed for real-time fax, users can run either a high-speed modem with speeds greater than 2400bps or a fax terminal in the VoIP channel. This capability provides a fallback for real-time fax transmissions. Both fax terminals and high-speed modems transmit a single tone when they answer a call, but each type of equipment uses a different tone. The TAOS unit detects the type of equipment in use on the basis of its answer tone. When it detects the equipment answering the call, the TAOS unit sends H.245 request-mode messages to request a switchover from the current audio codec to either G.711 with no echo canceler (for transparent modem) or T.38 data mode (for real-time fax).

Transparent data is encoded as an audio-mode type, either G.711 μ–law (64Kbps) or G.711 a-law (64Kbps). Real-time fax (if supported) is encoded as data-mode type T.38 fax.

Note Transparent data mode introduces an H.245 request-mode message that is not backward compatible with the real-time fax feature provided by pre-TAOS 8.0 releases. To interoperate with a MultiVoice Gateway using transparent mode, all TAOS systems should be upgraded to TAOS 10.0.

Limitation for low-speed modems

Real-time fax cannot be used concurrently with low-speed modems (2400bps or less) because low-speed modems use the same answer tone as fax terminals. If a low-speed modem is used on a VoIP channel that is enabled for real-time fax, the Gateway detects a fax answer tone and requests T.38 encoding. The ingress gateway (typically the gateway on which the modem call originated) can accept the T.38

encoding request or reject the request, which causes the egress gateway to terminate the call.

G711-Transparent-Data parameter

Configure the g711-transparent-data parameter in the voip profile:

```
[in VOIP/{ 0 0 }]
voip-index* = { 0 0 }
gatekeeper-ip = 135.92.52.138
gk-mlg-control = no
vpn-mode = no
single-dial-enable = no
packet-audio-mode = g729
frames-per-packet = 4
...
g711-transparent-data = no
...
```

The g711-transparent-data parameter setting enables or disables transparent transmission of fax or modem signals across VoIP channels. When enabled, if a MultiVoice Gateway detects a fax or modem Answer tone in a VoIP channel, the unit transparently requests end-to-end G.711 encoding and bandwidth for the call, in a process similar to that used by real-time fax. The echo cancelers are disabled when the TAOS unit enters this mode, thus providing transparent G.711 encoding. The data is encoded transparently as an audio-mode type, either G.711 μ–law (64Kbps) or G.711 a-law (64Kbps).

The g711-transparent-data parameter accepts the following values:

Value	Specifies
yes	A MultiVoice Gateway transparently requests end-to-end G.711 encoding and bandwidth for the call upon detection of a fax or modem Answer tone in a VoIP channel.
no	(The default) A MultiVoice Gateway continues with VoIP call processing, even when a fax or modem Answer tone is detected.

The following commands enable the transparent modem feature on VoIP channels:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set g711-transparent-data = yes
admin> write
VOIP/{ 0 0 } written
```

The following commands enable both real-time fax and the transparent modem feature for high-speed modems:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set g711-transparent-data = yes
```


S 1457

```
admin> list rt-fax-options
admin> set rt-fax-enable = yes
admin> write
VOIP/{ 0 0 } written
```

The g711-transparent-data parameter is N/A when either G.711 μ–law or G.711 a-law encoding is selected for the packet-audio-mode parameter (such as packet-audio-mode=g711-alaw).

Processing CED tones

A TAOS unit can detect two types of called station identification (CED) tones, fax and generic CED. Depending upon the type of CED tone detected, the TAOS unit will initiate a request for either transparent mode or T.38 fax mode.

The MultiVoice interface layer determines which mode to request on the basis of system configuration; initiating the request for the transparent mode or, when enabled, real-rime fax. This is possible when the g711-transparent-data parameter is enabled, the TAOS unit has been licensed for real-time fax, and the rt-fax-options parameter have been enabled.

```
voip { 0 0 }
rt-fax-options = { yes }
g711-transparent-data = yes
```

In this case, when fax CED is detected, the gateway sends an H.245 RequestMode message for real-time fax using T.38. When generic CED is detected, the gateway sends an H.245 RequestMode message for G.711 with no echo canceller. It initiates a Bandwidth Request (BRQ) for bandwidth of 64Kbps.

Caution Low-speed modems (<= 2400bps) use the same CED as fax terminals. Running a low-speed modem on a VoIP channel when real-time fax is enabled causes a the gateway to attempt a switch over to T.38 fax mode. If the ingress gateway (typically the fax/modem originate side) accepts the switch over request, then the VoIP call is changed to T.38. If the ingress gateway rejects the switch over then the call is terminated on the egress gateway.

If VoIP users run low-speed modems, then the gateway must be configured so that real-time fax is disabled and transparent data is enabled as follows:

```
voip { 0 0 }
rt-fax-options = { no }
g711-transparent-data = yes
```

Deactivating trunks used for VoIP calls

The trunk-quiesce-enable parameter enables MultiVoice Gateways to automatically deactivate trunks used for VoIP calls when a gateway becomes unavailable. When parameter value is yes, trunks configured to accept VoIP calls are made unavailable to the PSTN under the following conditions:

- A gateway cannot register with either a primary or secondary gatekeeper.
- A gateway's trunk connection with the PSTN is unavailable, so that gateway is forced to unregister itself from its gatekeepers.

Previously, when a Gateway could not register with the primary and secondary gatekeeper, the caller heard a fast-busy signal because the PSTN switch continued to

route calls to the trunks on that gateway. Deactivating the trunk changes the trunk state to inform the PSTN switch that those trunks are not available and forces the gateway to unregister from all known gatekeepers.

When the TAOS unit becomes unregistered, the gatekeepers route new calls to other gateways. Calls already in progress remain active until they are terminated by the caller or PSTN. When any one of the gateway's trunks comes back in service, that gateway starts registering itself with one of its gatekeepers. The gatekeeper then begins to route calls to this gateway.

Note System-wide deactivation can occur only on T1 trunks that use ISDN PRI signaling and have been configured for VoIP.

Enabling the trunk-quiesce-enable parameter

The `trunk-quiesce-enable` parameter enables automatic trunk deactivation whenever a MultiVoice Gateway is unable to register with either a primary or secondary MVAM, or force a MultiVoice Gateway to unregister whenever the trunk connection to the PSTN is unavailable.

Assigning the value yes to the `trunk-quiesce-enable` parameter causes the MultiVoice Gateway to be unavailable to accept calls whenever it becomes unregistered or it looses the connection to the PSTN. Assigning the value no, the default, allows it to continue processing call requests when unregistered or its PSTN connection goes down.

The following commands enable trunk deactivation for T1 PRI lines configured for VoIP:

```
admin> read voip { 0 0 }
VOIP/{ 0 0 } read
admin> set trunk-quiesce-enable = yes
admin> write
VOIP/{ 0 0 } written
```

Configuring PSTN call signaling

An egress MultiVoice Gateway can manage call signaling with the switched network by:

- Enabling transparent delivery of Q.931/Q.850 cause codes received from the PSTN by the far-end MultiVoice Gateway to the near-end MultiVoice Gateway
- Enabling configuration of the bearer capabilities sent in the Q.931 Setup message by the far-end MultiVoice Gateway for outbound calls to the switched network
- Enabling configuration of reporting the Q.931 Progress Indicator information element (IE) in the Proceeding and Alerting message by the near-end MultiVoice Gateway to the switched network configurable

MultiVoice call signal processing made is consistent with the following telecommunications standards:

- ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1) - ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993), International Telecommunications Union
- ITU Telecommunication sector standard (ITU-T) Q.850, *Usage of Cause and Locations in the Digital Subscriber Signalling (sic) System No. 1 and the Signalling (sic) System No. 7 ISDN User Part* (Mar. 1993), International Telecommunications Union

Transparent reporting of disconnect cause codes

MultiVoice provides transparent reporting of call disconnect cause codes for both the far-end MultiVoice Gateway and near-end MultiVoice Gateway using Q.931 (H.323) or Q.850 (SS7) signaling.

If the inbound PSTN connection uses PRI signalling when a VoIP call is disconnected, the near-end MultiVoice Gateway passes the Q.931 disconnect message—generated by the far-end PSTN and passed across the packet network by the far-end MultiVoice Gateway—directly to the near-end switched network. When the Q.931 disconnect message is received by the local telephone company switch, it plays the appropriate tone for the caller. The near-end MultiVoice Gateway does not play any voice announcement or tones.

If the inbound PSTN connection uses inband signalling, or the call is disconnected internally, the near-end MultiVoice Gateway responds to the Q.931/Q.850 cause codes, reporting the information to the MVAM. Then the near-end MultiVoice Gateway generates either the appropriate call-progress tone or voice announcement for the caller, depending upon the instructions it receives from MVAM.

With transparent reporting of call disconnect cause codes disabled, when a VoIP call is disconnected the near-end MultiVoice Gateway plays the appropriate voice announcement or tones for the end user. Then the near-end MultiVoice Gateway sends Q.931 disconnect message with cause code NORMAL (16). to the local telephone company switch.

Configuring bearer capabilities for outbound calls to the PSTN

An egress MultiVoice Gateway can be configured to request a specific bearer service from the switched circuit network for outbound VoIP calls. The MultiVoice Gateway can be configured to request the following bearer services from the egress switched telephone network for outbound call processing:

- Speech
- Unrestricted digital information
- Restricted digital information
- 3.1 kHz audio
- Video

Request for a specific bearer service is transmitted to the switched telephone network in the bearer service information element of the call-setup message sent by the MultiVoice Gateway. For more information see "4.5.5 Bearer capability" in ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1)—ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993). The bearer service request is configured through the TAOS administration interface. Prior to TAOS 10.0, the egress MultiVoice Gateway always requested "speech" bearer service when connecting a VoIP call to the switched telephone network.

Q.931 Call signaling progress indicator

An egress MultiVoice Gateway can be configured to forward the Q.931 progress indicator information element as part of the Alerting and Proceeding message sent to the ingress switched network. The Q.931 progress indicator information element

describes call routing events on the egress switched telephone networks used for a VoIP call.

When use of the progress indicator information element is enabled, a MultiVoice Gateway includes the call routing event descriptions in the Alerting and/or Proceeding messages sent to the ingress switched network. The progress indicator information element reports one of the following routing conditions:

- Call is not end-to-end ISDN; further call-progress information may be available in-band.
- Destination address is non-ISDN.
- Origination address is non-ISDN.
- Call has returned to the ISDN.
- Interworking has accused and has resulted in a telecommunication service change.
- In-band information or an appropriate pattern is now available.

For more information on the use of the progress indicator information element, see "4.5.23 Progress Indicator" and "Annex G" in ITU Telecommunication sector standard (ITU-T) Q.931, *Digital Subscriber Signalling (sic) System No. 1 (DSS 1)—ISDN User-Network Interface Layer 3 Specification for Basic Call Control* (Mar. 1993).

Detecting and reporting call-progress

To detect progress indicators in call alerting and proceeding messages on a near-end MultiVoice Gateway, inbound VoIP calls from the switched telephone network must be differentiated from non-VoIP calls (such as, analog).

When using inband signaling, the `default-call-type` parameter in the `t1:line-interface` or `e1:line-interface` sub-profile specifies what call-type the MultiVoice Gateway should expect for incoming calls on this trunk, for purposes of call routing. The `default-call-type` parameter applies to inband and PRI signaling for VoIP calls. Set `default-call-type=voip` to enable sending the progress indicator in call alerting and proceeding messages for PRI signaling.

pstn-attribute subprofile

This feature adds the `pstn-attribute` subprofile to the `voip` profile. This profile contains the following parameters:

```
admin> list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
cause-code-transparency = no
alert-progress-indicator = no-progress-indicator
proceed-progress-indicator = no-progress-indicator
bearer-capability = speech
```

cause-code-transparency parameter

The `cause-code-transparency` parameter in the `pstn-attribute` sub-profile of the `voip` profile enables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network—passed across the packet network from the far-end MultiVoice Gateway to the near-end MultiVoice

S 1461

Gateway—to the local telephone company. The local telephone company switch then plays the appropriate tone or disconnect message for the caller.

The cause-code-transparency parameter may be assigned the following values:

Parameter value	Specifies
yes	Enables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network to a local telephone company switch, across a MultiVoice network. The local telephone company switch responds to these messages by playing the appropriate tones or messages for the caller.
no	(The default) Disables transparent delivery of the Q.931 (H.323 VoIP) or Q.850 (SS7) disconnect cause codes generated by the far-end switched network to a local telephone company switch, configuring the near-end MultiVoice Gateway to play the appropriate tones or messages for the caller.

Changes to the cause-code-transparency parameter take effect with the next VoIP call. The following example illustrates how to enable transparent delivery of disconnect cause codes:

```
tnt132>read voip { 0 0 }
VOIP/{ 0 0 } read

tnt132>list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
cause-code-transparency = no
....

tnt132>set cause-code-transparency = yes

tnt132>write
VOIP/{ 0 0 } written
```

The cause-code-transparency parameter has the following dependencies:

- This parameter should be enabled (cause-code-transparency=yes) whenever voice announcement reporting is enabled (h323-voice-ann-enabled = yes), for callers to hear both a busy signal and the call failure message. When voice announcements are enabled, if transparent delivery of disconnect codes is disabled (cause-code-transparency=no), callers do not hear the busy tone. Instead, the near-end MultiVoice Gateway plays the call failure message.

alert-progress-indicator parameter

The alert-progress-indicator parameter in the pstn-attribute sub-profile of the voip profile configures the type of call-progress events that are captured and reported in the Q.931 Alert message progress indicator information element by the MultiVoice Gateway. Once configured, MultiVoice Gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

The `alert-progress-indicator` parameter may be assigned the following values:

Parameter value	Specifies
`no-progress-indicator`	(The default) Disables alert reporting of call routing events on the egress switched telephone network.
`none-end2end-isdn`	The egress MultiVoice Gateway reports when calls are connected to a egress switched telephone network which does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF signaling.
`dest-non-isdn`	The egress MultiVoice Gateway reports when calls are connected to a egress switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not return call-progress signals to the MultiVoice Gateway.
`orig-non-isdn`	The ingress MultiVoice Gateway reports when calls are received from a local switched telephone network which does not use ISDN signaling, such as a transit network or private network, which does not provide call-progress signals to the MultiVoice Gateway.
`return-to-isdn`	The egress MultiVoice Gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.
`interworking-occurred`	The egress MultiVoice Gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
`inband-info-available`	The egress MultiVoice Gateway reports if inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

The following example illustrates how to set the parameter for reporting calls that are connected to a far-end switched telephone network that does not use ISDN signaling:

```
tnt132>read voip { 0 0 }
VOIP/{ 0 0 } read
```

```
tnt132>list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
....
alert-progress-indicator = no-progress-indicator
....
tnt132>set alert-progress-indicator = none-end2end-isdn
tnt132>write
VOIP/{ 0 0 } written
```

Changes to the `alert-progress-indicator` parameter take effect with the next VoIP call.

proceed-progress-indicator parameter

The `proceed-progress-indicator` parameter, in the `pstn-attribute` sub-profile of the `voip` profile, configures the type of call-progress events that are captured and reported in the Q.931 Proceeding message progress indicator information element by the MultiVoice Gateway. Once configured, MultiVoice Gateways report when specific call routing events occur for VoIP calls passing from the packet network and the switched telephone network.

The `alert-progress-indicator` parameter can be assigned the following values:

Parameter value	Specifies
`no-progress-indicator`	(The default) Disables alert reporting of call routing events on the egress switched telephone network.
`none-end2end-isdn`	The egress MultiVoice Gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling. The egress switched telephone network may support robbed-bit or detectable DTMF signaling.
`dest-non-isdn`	The egress MultiVoice Gateway reports when calls are connected to an egress switched telephone network that does not use ISDN signaling, such as a transit network or private network, that does not return call-progress signals to the MultiVoice Gateway.
`orig-non-isdn`	The ingress MultiVoice Gateway reports when calls are received from a local switched telephone network that does not use ISDN signaling, such as a transit network or private network, which does not provide call-progress signals to the MultiVoice Gateway.
`return-to-isdn`	The egress MultiVoice Gateway reports when calls connected across a transit network are routed back on to trunk supporting ISDN signaling.

S 1464

Parameter value	Specifies
interworking-occurred	The egress MultiVoice Gateway reports if interworking occurs upon connecting a call to the switched telephone network. Such events occur when the selected bearer capability is not supported or when a resource or route with the preferred capability is not available.
inband-info-available	Assigning this value, the egress MultiVoice Gateway reports if inband call-progress signaling or other supported non-ISDN signaling is available from the switched telephone network for the connected call.

The following example illustrates how to set the parameter to report calls that are proceeding on a far-end switched telephone network that does not use ISDN signaling:

```
tnt132>read voip { 0 0 }
VOIP/{ 0 0 } read
tnt132>list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
....
proceed-progress-indicator = no-progress-indicator
....
tnt132>set proceed-progress-indicator = none-end2end-isdn
tnt132>write
VOIP/{ 0 0 } written
```

Changes to the proceed-progress-indicator parameter take effect with the next VoIP call.

bearer-capability parameter

The bearer-capability parameter, in the pstn-attribute sub-profile of the voip profile, configures the request for a specific bearer service from the egress switched circuit network for outbound VoIP calls. The request is transmitted to the switched telephone network in the bearer service information element of the call-setup message sent by the MultiVoice Gateway.

The bearer-capability parameter may be assigned the following values:

Parameter value	Specifies
speech	(The default) Requests a switched network routing over a channel that supports speech bearer capability.
unrestricted-digital-info	Requests a switched network routing over a channel that supports unrestricted digital information (UDI) bearer capability.

S 1465

Parameter value	Specifies
restricted-digital-info	Requests a switched network routing over a channel that supports restricted digital information (RDI) bearer capability.
audio-3100hz	Requests a switched network routing over a channel that supports digital audio bearer capability up to 3.1kHz.
video	Requests a switched network routing over a channel that supports video signaling bearer capability.

The following example illustrates how to specify digital audio bearer capability for VoIP calls:

```
tnt132>read voip { 0 0 }
VOIP/{ 0 0 } read
tnt132>list pstn-attribute
[in VOIP/{ 0 0 }:pstn-attribute]
....
bearer-capability = speech
tnt132>set bearer-capability = audio-3100hz
tnt132>write
VOIP/{ 0 0 } written
```

Changes to the bearer-capability parameter take effect with the next VoIP call.

Multiple Logical Gateways

TAOS implements dynamic call control for H.323 VoIP calls on MultiVoice networks and provides support for partitioning a single MultiVoice Gateway into multiple logical gateways. Using this method of call control lets the H.323 Gatekeeper perform call-specific administration on a call-by-call basis.

Call-specific administration of H.323 VoIP calls is allowed for the following call control functions on the same physical MultiVoice Gateway:

- PIN prompting
- Single-stage dialing
- Two-stage dialing
- Voice announcement playback
- Configurable call timers for prepaid and credit card billing systems

MVAM analyzes call performance data (trunk group, DS0 status, and call activity) received when a gateway performs periodic keepalive registration. When MVAM responds to subsequent call requests from each gateway, the Administration Conformation (ACF) message includes any changes defined for the aforementioned call administration parameters. The gateway applies the parameter changes received from MVAM to the current call request. This information is stored as part of the nonstandard data included in registration, admission and status (RAS) messages exchanged by the gateway and gatekeeper for each call.

Caution Dynamic call control and multiple logical gateways are only supported in MultiVoice networks running TAOS 10.0 on the gateways and MVAM 3.0 on the gatekeepers. These features are not supported in MultiVoice networks where gatekeepers are running Release 2.x of MVAM.

MVAM 2.x configures all H.323 call management features globally, on each MultiVoice Gateway, using the values assigned in the Voip Options profile. A gatekeeper running MVAM 3.0 can send instructions to the ingress gateway which override global call management settings utilizing status information reported by MultiVoice Gateways. The decision to override the global call management settings can be based upon reported ingress trunk or DS0 groups, Caller ID, time-of-day, gateway, etc.

The rules used to apply overrides to H.323 call management parameters are configured on MVAM. These parameter changes are useful when partitioning MultiVoice Gateways into logical gateways. *Logical gateways*, defined on MVAM, treat selected trunk groups on a MultiVoice Gateway as if they were a unique VoIP gateway. Initially, MultiVoice Gateways must have T1, T3 and PRI trunks to support logical gateways.

Note While BRI lines can still be used for VoIP, the multiple logical gateway features are not supported on MultiVoice Gateways that use BRI.

A MultiVoice Gateway cannot identify its own logical gateways. Only the gatekeeper running logical gateways can identify the MVAM. However, a gateway must be configured to apply instructions received from MVAM when processing the current call.

H.323 Call-specific administration

H.323 call-specific administration lets MVAM override defaults for PIN authentication, dialing mode and voice announcement playback.

MVAM can enable call-specific administration on the basis of the reported DNIS, ANI, trunk group and DS0 information, or any combination of that data, which are all reported in the first ARQ from the gateway.

Dynamic PIN authentication

When multiple logical gateways are enabled on a MultiVoice Gateway, any incoming call request immediately sends an ARQ to MVAM that include the following information:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM sends an ACF message to the gateway. The gateway then processes the call as if the following VoIP parameters were set to these values:

```
vpn-mode=yes
single-dial-enable=yes
```

If MVAM or a third-party billing application used with MultiVoice requires PIN authentication for the call, an Admission Reject (ARJ) message is issued directing the gateway to set vpn-mode=no for this call. The gateway then resumes call handling as if

the call had just arrived from the PSTN but prompts for authentication (as if vpn-mode=no) before continuing with call processing.

Dynamic single-stage and two-stage dialing

When the multiple logical gateways are enabled on a MultiVoice Gateway, any incoming call request immediately sends an ARQ to MVAM that includes the following information:

- DNIS, when available
- ANI, when available
- Trunk group and DS0 status changes

If the ARQ includes all the information necessary to route the call, MVAM sends an ACF message to the gateway. The gateway then processes the call as if the following VoIP parameters were set to these values:

```
vpn-mode=yes.
single-dial-enable=yes
```

If MVAM or a third-party billing application used with MultiVoice requires a caller perform two-stage dialing for this call (dialing the destination telephone number after dialing into the MultiVoice Gateway), an Admission Reject (ARJ) message is issued directing the gateway to set single-dial-enable=no for the call. The gateway will then resume call handling as if the call had just arrived from the PSTN, but prompt the caller to enter the destination telephone number (single-dial-enable=no) before continuing with call processing.

Static announcement branding

When the multiple logical gateway feature is enabled on a MultiVoice Gateway, MVAM or a third-party billing application can select a set of voice announcements for playback from multiple sets of voice announcements stored on the gateway. This is known as *branding*.

By sending either an ARJ or ACF message containing an announcement directory specifier, the gateway plays voice announcements from the named directory on the PC flash card for the current call.

Executing the branding instructions, the gateway searches for the voice announcement directory using the value set in the voice-ann-dir parameter. When voice-ann-dir=/current (default) and MVAM requests a specific directory (brand) of announcements for a call, the gateway searches for those announcements starting in the /current directory. For example, if MVAM specifies italian, the gateway searches for announcements in the directory /current/italian/.

Note It is recommended that you use only four brands of static announcements because there are limitations in the announcement cache size. Using more than four brands degrades announcement quality and overall gateway performance.

Configurable call timers

MultiVoice supports the use of configurable call timers, controlled by MVAM or a third-party billing application that supports timed billing plans (such as prepaid phone cards or prepaid cellular accounts).

S 1468